STATEMENT OF WORK

FOR

AMES RESEARCH CENTER (ARC)
AMES CONSOLIDATED INFORMATION TECHNOLOGY SERVICES (ACITS) 3

NNA10301939R

20 August 2010

C.1 INTRODUCTION

NASA Ames Research Center, commonly referred to as Ames, or ARC and located at Moffett Field, California, was founded December 20, 1939, as an aircraft research laboratory by the National Advisory Committee for Aeronautics (NACA). In 1958, Ames became part of the National Aeronautics and Space Administration (NASA). Ames is located in the heart of California's Silicon Valley at the core of the research cluster of high-tech companies, universities and laboratories that define the region's character. With over $3.0 billion in capital equipment, 2,300 research personnel, and a $600 million annual budget, Ames' economic impact is significant. Ames plays a critical role in virtually all NASA missions in support of America's space and aeronautics programs as well as information technology (IT), nanotechnology, fundamental space biology, biotechnology, aerospace and thermal protection systems, human factors, astrobiology, and Federal Aviation Administration (FAA) air traffic management research. Further information on the ARC mission and its contribution to the NASA vision can be obtained from the web site http://www.arc.nasa.gov.

As a leader in information technology research with a focus on supercomputing, networking, and intelligent systems, Ames conducts the critical research and development (R&D) and develops the enabling technologies that make NASA missions possible.

To accomplish its mission, the Center depends heavily on state-of- the-art IT, embracing computer systems ranging from laptop and desktop personal computers to mid-range computers and supercomputers; network systems ranging in size and complexity from those supporting individual buildings up to and including those serving the entire Ames facility; data storage facilities ranging in size from compact disks to massive, centrally-accessed tape storage systems; and all of the associated operating, input/output, data transfer, data management, and data analysis systems.

NASA's focus on science and discovery requires innovation at all levels, including IT services. Ames is already a demonstrated Agency IT leader in the areas of high performance networking, cloud computing, security, and web technologies. To maintain these leadership positions, and to secure other Agency IT support roles, a constant focus on innovation is required by the Contractor's management and employees. Ames' expectation is that its IT support contractor will make innovation a core component of every task executed under the ACITS 3 contract.

It is expected that cloud computing will continue to be an area of emphasis for Ames. As such, on-going R&D will be required maintain the Center's current leadership position and to continually deliver new cloud capabilities that are suitable for addressing NASA's unique mission challenges. In most cases, the innovation involving NASA cloud services will focus on providing solutions that the commercial marketplace cannot address due to the unique needs of NASA's missions. Some examples of areas needing innovative solutions to meet NASA's needs are the management of massive data storage capacities, very high performance networking, and security. In short, Ames will not simply operate a cloud-computing environment for NASA but instead will drive cloud computing innovation within the Federal Government, especially as it can be applied to address science challenges. It is expected that ACITS 3 will facilitate this path for Ames by providing the highest-caliber expertise available in cloud computing technologies.

C.2 SCOPE

Currently, the Outsourcing Desktop Initiative for NASA (ODIN) and the Ames Consolidated IT Services 2 (ACITS 2) contracts provide desktop computing, networking, telecommunications, and data center capabilities to Ames. In general, the ODIN contract provides a broad range of general-purpose end user support services including system administration, hardware and software maintenance, and help desk assistance. The ODIN approach is designed to offer a comprehensive, end-to-end desktop service for those systems that are considered to be fully functional and mature and provides an operational system that is stable.

ODIN will continue to be the default provider of end user IT services (such as, desktops, laptop, cell phones, and pagers) for the majority of ARC IT systems. The ACITS 3 contract, on the other hand, will provide, a wide range of support functions, including those for non-standard operating systems, system interfaces, or for use within a dynamic environment such as a research laboratory or test facility. These functions include but are not limited to computing support services (including system administration, hardware and software maintenance, and development of new software applications or modification of existing software to change or add to its functionality) for systems that are either uniquely configured or highly specialized in function and that do not provide office automation services for end users. Some of these capabilities may be re-assigned to the I^{3}P contracts (Agency Consolidated End User Services, or ACES, which will supplant ODIN, after its award; NASA Integrated Communications Services, or NICS; Enterprise Application Service Technologies, or EAST; Web Enterprise Service Technologies, or WEST; and NASA Enterprise Data Center, or NEDC) as they are awarded. The ACITS 3 contract will continue to provide services that are not covered by either the ODIN or I^{3}P contracts, including but not limited to, IT capabilities and expertise for research, engineering, maintenance, and operations.

The Intelligent Systems Research and Development (ISRDS) contract is another existing Ames contract vehicle which provides IT support to Ames. The ISRDS contract provides fundamental research, development, and infusion support services for code TI projects and programs. In contrast, the ACITS 3 contract will provide IT capabilities and expertise in support of applied research, engineering, maintenance, and operations for the Center and the Agency.

ACITS 3 services fall into the following categories (as stated in section 3.0 in further detail):

- IT Systems & Governance Support
- IT Security Support
- Network and Communication Systems & Support
- Application Management & Support
- Scientific Computing Systems & Support
- Innovation and Emerging Technologies
- Outreach/Informational Systems & Support

- Management and Administration

Work requirements for ACITS 3 will be furnished by the Government through the issuance of task orders (TOs). Technical performance standards and metrics will be provided in the TOs.

Software development, operations, and maintenance under ACITS 3 apply to software at several levels of risk and control from minimal to critical (as it relates to impact to the Government) that will be specified by the Government in TOs.

The Contractor shall furnish all personnel, training, facilities, and specialized equipment not provided by the Government as part of a TO, and those materials and transportation necessary to perform these services. For on-site Contractor staff, the Government shall establish an arrangement with the ARC ODIN or ACES contractor and provide all on-site Contractor desktop computers and services for equipment requiring access to the NASA internet protocol (IP) space. Any on-site Contractor-provided equipment connected to the NASA IP space shall require an approved waiver, as provided by the Chief Information Officer (CIO), and shall comply with NASA Information Technology Requirement NITR-2830-1, Networks in NASA IP Space or NASA Physical Space.

While the majority of work is directly in support of Ames Research Center, other Centers within the Agency and Government partners of ARC are at times supported. This support may be provided at remote sites.

In the performance of this SOW the Contractor may be required to support IT projects that are subject to the scope of NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements. When such requirements are specified as part of a TO, the Contractor shall comply with NPR 7120.7 as applicable.

The Contractor shall determine, subject to Government approval, the most appropriate method to connect devices from offsite and near-site facilities that require connectivity to resources on ARCLAN (NASA IP Address space). The first option the contractor shall have available to it is to extend the ARCLAN perimeter to include the offsite facility. This option requires that IT resources on the Government Furnished Equipment GFE network (including but not limited to all desktops, laptops, and workstations, all cabling, all routers and switches, and other IT resources) be managed and operated by the Government or its service provider. No Contractor IT resources will be allowed to connect to the GFE network if this option is chosen. The second option the contractor shall have is to utilize the NASA Ames client-to-network virtual private network (VPN) system.

C.3 MISSION FUNCTIONS AND MANAGEMENT AND ADMINISTRATION

C.3.1 Mission Functions

C.3.1.1 IT Systems and Governance Support

C.3.1.1.1 Project Management

The contractor shall comply with all Project Management Office (PMO) requirements, methodology, and best practices. The contractor will manage projects within the defined methodology of the Lite/Medium/Full NPR 7120.7 frameworks as applicable. The contractor shall develop project plans, schedules, risk analysis, stakeholder management, communications management, and other applicable documents for the PMO.

C.3.1.1.2 System Administration

The Contractor shall provide products and services in order to maintain a stable, efficient, and productive computer system and computing environment. These activities include system software maintenance and updates, ensuring compliance with Center Information Technology (IT) security requirements, user account management, configuration management, system upgrade and improvement, computing operations, maintenance of systems documentation and procedures, and contingency planning.

C.3.1.1.3 Data Center

The ARC Data Center is currently comprised of facilities in buildings N233, N254, M16, and a Container implementing state of the art cloud technology; it is expected that the location and number of facilities will be dynamic over the life of the ACITS 3 contract. These facilities enable ARC to provide infrastructure, Mission, Agency, and Government-wide services with outstanding availability and reliability.

The contractor shall ensure that best practices and lessons learned, such as Gartner and ITIL, are implemented and maintained in the ARC Data Centers. The Contractor shall manage both the environmental conditions (including, but not limited to, power, HVAC, UPS, backup generators, and PDUs) and the IT equipment (including, but not limited to, servers, backup, cables, network connections, and storage systems). In this capacity the contractor is responsible for diverse efforts, including, but not limited to, operations, configuration management, installing and testing new equipment, monitoring all systems including IT and environmental equipment, specialized cleaning of the IT facilities as required, documentation, development of standard operating procedures (SOPs), access control, cable management, and capacity planning and management.

The technology and specific systems and requirements necessary to provide optimal support to the data centers are expected to change over the lifetime of this contract. The contractor shall have a thorough knowledge and extensive experience in all current emerging technologies relative to data centers (e.g., virtual systems, cloud computing, and the “green initiative”). The contractor shall provide ARC with the benefit of its experience and expertise in relevant emerging technologies.

C.3.1.1.4 Facility Support

The Contractor shall provide technical and administrative support to specific IT facilities and infrastructure that require environmental controls, regulation, and/or conditioning above and beyond what an average professional office complex would provide.

C.3.1.1.5 Hardware/Software Maintenance

The Contractor shall provide for the repair and replacement of hardware components and software modules, applications, and systems necessary to ensure the operability of all covered computing and communication systems. Supporting functions include problem diagnosis;, repair or replacement of failing or failed components; verifying that components, modules, and applications meet applicable standards; system performance testing and verification; data integrity and restoration; and an understanding of applicable security considerations regarding sensitive or classified data or systems.

C.3.1.1.6 Data Storage Retrieval and Archival

The Contractor shall provide the IT systems and related services necessary to store and maintain reliable and secure access to large amounts of electronic data. Technical areas of focus include systems engineering, deployment, and operations; storage for near-term, long-term, and archival requirements; shared access and security features; data integrity; backup systems; disaster plans; user interface and access systems; identification of potential sources for required products and services; and assessment of relevant emerging technologies and technical approaches.

C.3.1.1.7 IT Governance and Policy Analysis

The contractor shall provide IT Governance and policy analysis with regards to existing policies, procedures, and guidelines, and their impact to Center Operations and services.

The contractor shall comply with all Federal, NASA, and Center level policies, procedures, standards, and guidelines pertaining to Federal records management as applied to Federal systems.

C.3.1.1.8 Technical Planning and Analysis

The Contractor shall provide technical support in the conduct of IT-related technical planning associated with IT resources management; planning for new IT systems and IT facilities; definition of near- and long-range IT requirements; and evaluation of new standards, practices, and policies. The contractor shall provide administrative and technical support for all IT planning and management activities, including, but not limited to, Capital Planning and Investment Control (CPIC), Enterprise Architect (EA), website registration, summary investment business cases, data calls, privacy, Section 508, waiver tracking and reporting, IT asset management support, and integration of EA and IT portfolio management. The contractor shall build and maintain an integrated EA system relative to all EA services. The Contractor shall provide technical resources to support engineering analysis and evaluation of new IT concepts, technologies, architectures, and systems; definition of functional requirements and synthesis of IT systems requirements; identification of relevant solutions, systems, and products; and development of cost/benefit estimates.

C.3.1.1.9 Records Management and Vital Records Management for Continued Operations

The Contractor shall provide for the design, development, installation, maintenance, operations, upgrades, configuration management, archiving, customer support, training, and security of electronic records systems and related applications, including tracking systems for technical reports and data.

The Contractor shall provide technical support and coordination to ensure effective and efficient Records Management and Vital Records Management, including, but not limited to, entering records into the system, reviewing policies and procedures, supporting day-to-day operations, and archiving records.

C.3.1.2 IT Security

The Contractor shall be responsible for the maintenance and operations of the ARC Institutional IT Security Systems including firewalls, intrusion detection and prevention, IT security support systems, vulnerability and patch management, incident response and forensics, log aggregation, and correlation.

The contractor shall comply with all Federal, NASA, and Center level policies, procedures, standards, and guidelines pertaining to IT security as applied to Federal systems.

The contractor shall provide needed support in the area of cyber laws and ethics. The contractor shall have access to a subject matter expert (e.g. onsite, or reach back within the company or through a subcontractor or partner) in the domestic and international cyber laws.

C.3.1.2.1 Patch Management and Deployment

The contractor shall operate, maintain, monitor, and push patches via the Agency-approved patch management tool. The contractor shall ensure that knowledgeable staff is involved with monitoring of the Patch Management tool to ensure that the latest vulnerabilities are being included by the vendor and that patches are being properly tested and deployed. The contractor shall address any gaps with alternate mitigating tools.

C.3.1.2.2 Vulnerability Scanning Systems

The Contractor shall operate, maintain, and monitor the Vulnerability Scanning Systems consisting of hardened scanners fixed or rendered mobile to perform vulnerability, network discovery, certification and accreditation (C&A), ad hoc, wireless, and perimeter scanning. The Contractor shall assist with periodic scanning report creation using scripting and data correlation. The Contractor shall maintain knowledge of ARC networks, research the unique properties of vulnerabilities affecting widely installed software, and optimize the scanner configuration in order to minimize disruption of daily operations for targeted systems and to minimize false positives and false negatives.

The Contractor shall also conduct scans of the ARC network and campus (including Numerical Aerospace Simulation (NAS) and National Research and Education Network (NREN)), such as network discovery scans, vulnerability scans, ad hoc scans, network perimeter scans, and wireless scans. The Contractor shall coordinate with ARC organizations to remediate vulnerabilities and perform follow-up scans to validate remediation.

The Contractor shall conduct ad hoc vulnerability and configuration scanning of systems or websites to assess risk of IT security threats before attaching a system or website to the ARC network.

C.3.1.2.3 Intrusion Detection and Intrusion Prevention

The contractor shall provide intrusion detection and prevention specialists, with some focus on deep Transmission Control Protocol (TCP) analysis and in-line skills to perform inline patching at the network level whenever possible. The Contractor shall maintain knowledge of monitored systems and research the unique properties of suspicious traffic in order to write effective signatures to exclusively detect and prevent malicious or unauthorized activity unique to ARC.

C.3.1.2.4 Incident Response Life Cycle

The Contractor shall participate in IT security incident response through membership on the ARC Incident Response Team as defined by the ARC IT Security Incident Response Plan. The Contractor shall provide as-needed, on-call IT security incident response 24 hours per day, 7 days a week.

The Contractor shall participate with system personnel (both civil service and contractor) when responding to an incident.

The Contractor shall provide detailed documentation of actions taken and the conclusions drawn from analysis. The Contractor shall protect all documentation and communications associated with incidents in accordance with Agency requirements for Controlled Unclassified Information (CUI) data at a minimum.

The contractor shall follow all phases of the IR lifecycle including:

- Preparation - plan a process for detecting and reacting to incidents per NASA’s needs;
- Detection - quickly and reliably obtain information to determine whether it is an event which threatens an organization’s security;
- Analysis - determine scope, impact, and severity to establish an appropriate response and develop a strategy to implement that response;
- Action - draft a detailed root cause analysis, execute forensics activities if necessary, and restore the system to operational state; and
- Postmortem - make recommendations and policy decisions to prevent future damage, and carry out any other post-incident actions.

C.3.1.2.5 Security Forensics

The contractor shall maintain qualified Security Programmers who possess C/C++/Assembly expertise to perform malware and binary analysis, packet deconstruction, flaw confirmation, and reverse engineering of code.

C.3.1.2.6 Certification and Accreditation Consulting and Auditing Support

The Contractor shall provide support to ARC organizations in performing their Certification and Accreditation (C&A) tasks and activities in accordance with NPR 2810.1 requirements. The Contractor shall:

- maintain an expert knowledge of all National Institute of Standards and Technology (NIST) and NASA requirements and understand their security implications in order to instruct ARC organizations on how to effectively implement security controls;
- possess a thorough understanding of NIST’s C&A processes in order to interpret policy, processes, and procedures;
- train ARC organizations on how to perform C&A activities;
- review the security controls of ARC IT Systems;
- assist ARC organizations with managing their C&A packages in the C&A repository;
- provide C&A repository training;
- critique C&A documentation and provide feedback to the owning organization;
- assist in performing pre-certification and perform Security Testing and Evaluation (ST&E);
- assist with certifications and/or audits by outside parties;
- perform audits to verify the completion of the Plan of Action and Milestone (POAM);
- consult with system owners or designees in their performance of continuous monitoring (security control testing);
- attend appropriate control boards as directed by the CO, reporting on the meeting results and making recommendations to the ARC Certification and Accreditation Official (CAO); and
- assist with contingency plan testing and testing of controls, plan writing and updating, and risk analysis and assessment.

C.3.1.2.7 Perimeter Firewall Systems

The Contractor shall operate, maintain, and monitor the ARC border firewall systems along with any subnet, project, or program level firewall. The Contractor shall perform configuration management of the ARC firewall systems, abiding by all existing ARC/Agency level procedures and policies.

C.3.1.2.8 Antivirus (AV) Services

The contractor shall support both existing AV solutions and actively seek new and advanced AV solutions that support virus, malware, and Trojan detection and mitigation. AV services features include single console, antivirus, antispyware, and malware detection, and reports generated to show compliance of enterprise computers by tracking definitions and products.

C.3.1.2.9 Host-Based Intrusion Detection and Prevention

The contractor shall be involved in the development, deployment and support of a center-level host-based Intrusion Detection System/Intrusion Protection System (IDS/IPS) that is capable of detecting known and unknown (zero-day) malware, viruses, local, and remote attacks. Host-based intrusion detection and prevention features to be fully supported include, but are not limited to, single console, firewall policies for allowing only acceptable network traffic, IPS policies that can be configured to determine if events are benign or malicious and that will allow events to be configured accordingly, application blocking feature that allows the blocking of specific or unknown programs, and application hooking that prevents unknown and potentially malicious applications from binding themselves to legitimate programs.

C.3.1.2.10 Content Monitoring & Filtering

The Contractor shall operate, maintain and monitor the ARC Content Monitoring and Filtering Systems, a suite of tools capable of filtering access to Internet and internal content made by ARC devices, caching content so as to reduce access latency, logging content access requests to support investigations and application troubleshooting, and detecting abuse of IT resources as defined by NASA and ARC Internet usage policies. Content Filtering Features shall include at a minimum:

- web filtering, including, but not limited to, web traffic, Instant Messaging, P2P traffic, and FTP sessions;
- scanning of downloads for viruses before they reach the desktop, including Contractor-provided licensing and hardware as required;
- web security to block malicious websites;
- policy control to permit or deny user access to resources based on location, function, or classification of data; and
- user racking and accountability.

C.3.1.2.11 Full Packet Capture and Flow Monitoring

The Contractor shall operate, maintain and monitor the full packet capturing and flow monitoring systems consisting of hardened sensors placed on secure monitoring segments with access to key areas of network infrastructure to collect flow and full packet capture information. The contractor shall provide staff expert in packet reconstruction and possessing full understanding of the TCP/IP stack.

C.3.1.2.12 Event Log Collection & Correlation

The Contractor shall operate, maintain, monitor, and tune the Consolidated Logging System consisting of a hardened central management console and fault-tolerant hardened data collectors placed on secure monitoring segments with access to key areas of network infrastructure to archive computer and network device logs, and tuned to avoid data loss. The Contractor shall maintain knowledge of monitored systems and research the unique properties of suspicious traffic to create alert conditions to exclusively detect malicious or unauthorized activity unique to ARC.

The Contractor shall operate, maintain, monitor, and tune the Security Information Management (SIM) Systems consisting of a hardened central management console and hardened sensors placed on secure monitoring segments with access to key areas of network infrastructure to provide continuous collection of network traffic directly and indirectly from institutional or organizational data sources (for example, Dynamic Host Configuration Protocol (DHCP) servers, Syslog servers, Domain Name System (DNS) servers, Active Directory Domain Controllers, and potentially any other IT Security System). The Contractor shall augment and enhance SIM capabilities to support new technologies, interpret data from new sources, and provide simpler, more intuitive operation. The Contractor shall support ad hoc report generation for data calls, IT Security incident response or auditing, and other information gathering activities using the SIM Application Programming Interface (API).

C.3.1.2.13 Network Access Control

The contractor shall support the development, deployment and support for a center level Network Access Control (NAC) infrastructure. The NAC infrastructure shall monitor the network for unauthorized and unauthenticated devices based off policy and group/user rights. The contractor shall be responsible for product testing and evaluation, including any bake-offs. The contractor shall also be responsible for deployment and ongoing operations of the NAC device, including tuning, policy definition, and maintenance.

C.3.1.2.14 Penetration Testing

The contractor shall participate in the development, implementation, and remediation of the IT Security Quarterly Penetration Testing Program and findings. The contractor shall have a thorough understanding of penetration testing through methods identified such as dumpster diving, social engineering, war-driving, and real world vulnerability exploitation.

C.3.1.2.15 Organization Computer Security Official (CSO) Support

The Contractor shall be responsible for performing Organization Computer Security Official (OCSO) tasks and activities as identified in NPR 2810.1, with the exception of determining policy and those tasks which are inherently Governmental.

C.3.1.2.16 Classified Security Collaboration

The contractor shall provide security support staff to work closely with the Center and Agency Office of Inspector General and Counter-Intelligence office on both non-classified and classified cases. The Contractor staff providing this support must maintain minimally a Secret Clearance, with some staff members being required to maintain a Top Secret clearance. The contractor may be required to also work closely with other Federal Agency entities, such as the Federal Bureau of Investigation (FBI).

C.3.1.2.17 Board Participation

The Contractor shall provide technical expertise at both formal and ad hoc board meetings. Examples of boards to be supported include the Network Access Control Board (NACB), the IT Project Management Board (PMB), the IT Customer Board, and other forums and working groups as required.

C.3.1.2.18 Remote Access Services

The Contractor shall operate and maintain remote access systems consisting of hardened Virtual Private Network (VPN) gateways using tunneling and proxy services to provide scalable, secure authentication and content encryption for thousands of remote users over the public internet. The Contractor shall create, test, and manage custom profiles against requirements to provide non-ARC personnel (e.g., foreign nationals, university researchers, and NASA personnel at other centers) secure access only to specific resources. The Contractor shall maintain multiple Secure Socket Layer (SSL) certificates for VPN gateways. The Contractor shall incorporate the use of improved authentication and encryption algorithms where appropriate. The Contractor shall perform Tier 2 troubleshooting to assist system administrators and users with the diagnosis and analysis of VPN problems.

C.3.1.2.19 IT Security Consultation and Engineering

The Contractor shall accept and respond to IT security-related requests by providing consultation and direct technical assistance to customers with the development of requirements for IT security solutions (e.g., designing firewall rules).

The Contractor shall support existing and new projects with qualified security and network engineers. IT Security Systems shall be engineered to ensure that safeguards for the protection of the confidentiality, integrity, and availability of unclassified IT resources are integrated into and support NASA’s missions, functional lines of business, and infrastructure based on risk-managed, cost-effective IT security principles and practices.

The Contractor shall execute the project plan by installing and integrating any system components as necessary into the existing network or lab environment. The Contractor shall document the system architecture (including diagrams), create or modify security plans, and write and electronically distribute user’s guides and operating procedures internally to Ames on an as needed basis.

C.3.1.2.20 Security Programming

The contractor shall provide qualified security programmers with expertise in Web 2.0, SQL, C, C++ and other programming languages to advise on current and emerging exploit vectors, database takeover, reverse engineering, and other pertinent programming and coding security threats.

C.3.1.2.21 Certifications

The contractor shall provide an IT security Subject Matter Expert who possesses at a minimum the following skills and certifications: ISC2 Certified Information System Security Professional (CISSP), SANS Global Information Assurance Certifications (GIAC), GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), Cisco Certified Network Engineer (CCNE), or equivalent network certifications (e.g., Certified Ethical Hacker (CEH)).

C.3.1.3 Network and Communication Systems and Support

The Network and Communication Systems and Support area is focused on operating, maintaining, managing, researching technologies for infrastructure improvement, and implementing changes to the infrastructure necessary to enable and enhance communications between human and computer customers and clients.

The Contractor shall define network requirements; identify potential sources for required products and services; maintain proficiency with legacy systems; assess new relevant technologies and technical approaches; recommend relevant solutions; estimate costs and benefits; and design, develop, deploy, and test hardware, firmware, and software systems.

C.3.1.3.1 Network Services

The Contractor shall provide for the installation, operation, management, monitoring, maintenance, repair, documentation, and upgrade of computer networks at the Center including local area networks, enterprise wireless networks, wide area networks, private networks, firewalls, and remote access services across a campus of approximately 80 NASA buildings and the NASA Research Park. The Contractor shall provide coordination with other NASA Centers, common telecommunication carriers, and commercial providers in support of external network links and services. The Contractor shall provide at least two senior level network engineers with Secret clearance to support IT Security Operations incident response. The Contractor shall provide network administrators and network engineers with Cisco Certified Network Administrator (CCNA) certification and Juniper Networks training. Contractor-provided network engineers shall possess current “Operating Juniper Networks Switches in the Enterprise” training.

C.3.1.3.2 Network and Communications Infrastructure

The Contractor shall provide support for the administration, configuration management, maintenance, documentation, and improvement of the network and communication infrastructure such as the underground and in-building cable plants utilized to provide communication services at ARC. These activities include engineering planning and design; installation and termination; maintenance of inventory and documentation; and testing, trouble-shooting, and repair. The Contractor shall provide coordination with other NASA Centers, common carriers, and commercial providers in support of external network links and services.

C.3.1.3.3 Distributed Systems

The Contractor shall provide for the installation, operation, management, monitoring, maintenance, repair, and upgrade of distributed systems, which generally consist of clusters of networked computers and other computer and communication equipment located at various sites throughout the Center.

C.3.1.3.4 Audio, Video, and Voice Communication Systems

The Contractor shall provide for the administration, operation, maintenance, repair, and installation of audio, video, and voice systems. The Contractor shall provide coordination with other NASA Centers, common carriers, and commercial providers in support of external network links and services.

C.3.1.3.4.1 Audio Systems

The contractor shall provide for the maintenance, repair, and installation of public address systems, auditorium audio systems, individual building intercom systems, and paging systems.

C.3.1.3.4.2 Video Systems

The contractor shall provide for the operation, maintenance, repair, and installation of surveillance systems; auditorium video systems; closed-circuit video; the Center's cable access television system; digital video systems coordination and integration; Direct Satellite Service; Ames Video Network VIDNET; video teleconferencing centers (VITS); desktop video conferencing; and the distribution of video signals via the Video Control Center across the campus as well as to and from the satellite ground stations.

C.3.1.3.4.3 Voice Communication Systems

The contractor shall provide for the operation, maintenance, repair, and installation of voice only teleconferencing (VOTS); PBX lines; non-switched phone lines; facsimile machines; digital telephone switching (PBX) systems; VoIP (Voice over IP) systems, voicemail services; telephone management systems; secure voice communication systems; operator services; message center services; and ARC telephone directory services.

C.3.1.3.5 Radio Frequency (RF) and Emergency Communication Systems

The contractor shall provide for the technical support, maintenance, and repair of wireless (e.g., Radio Frequency (RF) and optical) communication devices such as trunking radios and other wireless communication devices that are under the guidance of the ARC RF Spectrum Manager. The Contractor shall provide coordination with other NASA Centers, common carriers, and commercial providers in support of external network links and services.

Contractor-provided RF technicians shall have experience with high-powered RF transmissions systems, including, but not limited to, commercial/public safety Land Mobile Radio (LMR) repeater systems, High Frequency (HF) short wave and VHF/UHF transmission systems, and earth station satellite terminals (VSATs) and everything that comprises RF emission system antennas (e.g., antenna, cabling, amplifiers, grounding, and static discharge).

The contractor shall support the configuration control of all ARC-commissioned emergency communications systems as specified by either the ARC RF Spectrum Manager or Emergency Communications Manager. The contractor shall also confirm authorization with the ARC RF Spectrum Manager prior to transmitting on any frequency emission systems that directly support official federal government business on- or off-site of ARC. The contractor RF technicians shall maintain collateral Secret clearance to support Emergency Communications.

C.3.1.4 Application Management and Support

This area consists of IT applications management, business systems, and support required for the daily business processes and services necessary to operate the Center (e.g., financial services, human resources, IT and personnel security, logistics, and business system infrastructure).

Coordination and integration with current and future applications and business systems at the Center and across the Agency is critical to the efficient and effective operations of NASA in general. Specific business systems may be managed and operated from a single

NASA organization for the entire Agency, while other systems are managed and operated separately by each NASA Center.

The contractor shall maintain software developed under this contract. In general, the Contractor shall follow the maintenance process defined in IEEE/EIA Standard 12207, Systems and Software Engineering - Software Life Cycle Processes; however, the processes shall be tailored to the particular software package and applied with a rigor consistent with the software control class. Maintenance process requirements for the various classes of software will be further defined in a work authorization (WA) to be issued at TO start.

C.3.1.4.1 IT Support to Financial Services

The Contractor shall provide IT support for the design, development, implementation, modification, maintenance, and operation of software tools and applications that support accounting, finance, procurement, and payroll functions. The operation of software tools referred to in the prior sentence exclude office administrative functions.

C.3.1.4.2 IT Support to Human Resources, Personnel Security and Logistics

The Contractor shall provide IT support for the design, development, implementation, modification, maintenance, and operation of software tools and applications that support employee training, employee benefits, other human resource services, personnel security management, certificate management, cardkey and electronic access, logistics, and property management. The operation of software tools referred to in the prior sentence exclude office administrative functions.

C.3.1.4.3 IT Support to Business Systems and Infrastructure

The Contractor shall provide IT support for the design, development, installation, modification, maintenance, operations, upgrades, configuration management, and security of business systems databases, application servers, and web servers. The operation of software tools referred to in the prior sentence exclude office administrative functions.

C.3.1.4.4 Web Applications

The Contractor shall provide for the design, development, installation, maintenance, operations, upgrades, configuration management, archiving, customer support, and security for ARC websites and web applications. The operation of software tools referred to in the prior sentence exclude office administrative functions.

C.3.1.4.5 Collaborative and Information-Based Systems

The Contractor shall provide for the design, development, installation, maintenance, operations, upgrades, configuration management, archiving, customer support, and security for content-rich, IT based data systems, where team and project collaboration and work can be shared, along with embedded data capture utilizing eforms capability and providing a workflow engine. Examples include, but are not limited to, Sharepoint Collaboration Tool for team sites, business and scientific databases and collections, geographical information systems, and digital image archive and retrieval systems.

C.3.1.4.6 Application Management

The Contractor shall provide products and services to ensure that the suite of software applications in use by the Ames Research Center (ARC) user community are compatible within and across covered systems; are purchased, maintained, and upgraded in a cost effective and legal manner; and allow for effective communication between ARC customers and suppliers.

The Contractor shall provide products and services to ensure that that custom software is maintained and upgraded using documented processes that guarantee proper configuration control, traceability, and computing integrity.

C.3.1.4.7 Data Management and Analysis

The Contractor shall provide IT support that enables government management and analysis of business data (e.g., financial, HR, security, training, logistics, and procurement) and other useful information in support of Agency and Center business applications, projects, and programs. This area includes data warehouse management; database development and monitoring; data distribution, data archival and reporting; management information systems (MIS) dashboards; and developing and implementing tools and techniques for data mining and data delivery.

C.3.1.4.8 Application Testing

The Contractor shall support application testing by providing unit, system, end-to-end, and end user test plans and reports. The Contractor shall perform periodic testing of Center business applications against modifications in standard desktop configurations to mitigate any integration or configuration issues.

C.3.1.5 Scientific Computing Systems & Support

Scientific Computing consists of designing, developing, installing, modifying, configuring, operating, and maintaining software and computing systems in order to solve computationally intensive and/or complex engineering and scientific problems in support of ARC missions, programs, and projects.

General requirements include developing and supporting relevant software tools, their computing platforms, and user interfaces; creating models and algorithms and modifying them to be compatible with specific tools; analyzing models and computational integrity; data acquisition and analysis; computational analysis; tool integration; and maintaining legacy software and systems.

Current or future ARC mission areas, programs, and projects that this Statement of Work (SOW) include, but are not limited to, aircraft modeling and design, flight simulation, air traffic management simulation, tilt rotor, cockpit design, and headset design. During the life of this contract, TOs may be written to support similar work within the Center (by programs or organizations) that also falls within these IT areas. The Contractor shall provide subject matter experts with vast experience and expertise in these areas as needed.

The contractor shall maintain software developed under this contract. In general, the Contractor shall follow the maintenance process defined in IEEE/EIA Standard 12207, Systems and Software Engineering - Software Life Cycle Processes; however, the processes shall be tailored to the particular software package and applied with a rigor consistent with the software control class. Maintenance process requirements for the various classes of software will be further defined in a WA to be issued at TO start.

C.3.1.5.1 Scientific Applications

Areas in which support shall be required include, but are not limited to, the design, development, implementation, modification, integration, maintenance, and operation of software algorithms, tools, and applications that address complex and/or computationally intensive scientific and engineering problems.

C.3.1.5.2 Data Acquisition & Analysis

Areas in which support shall be required include, but are not limited to, acquiring and analyzing data and other useful information in support of ARC missions, programs, and projects. This includes data acquisition, exchange and/or translation, reduction, distribution, and archival; the development and use of data analysis and visualization tools and techniques; and other types of computational analysis.

C.3.1.5.3 Modeling & Tool Development

Areas in which support shall be required include, but are not limited to, creating accurate representations in time and/or dimensional space of scientific phenomena, aerospace systems, and other physical systems and developing software tools to assist human operators in the performance of complex tasks. This includes algorithm development; surface and multi-dimensional modeling; the integration of computational software and/or systems with physical systems; real time simulations; user interface design, development, implementation, and integration; and tool design, development, implementation, and integration.

C.3.1.6 Innovation and Emerging Technologies

NASA's focus on science and discovery requires innovation at all levels, including IT services. The ACITS 3 contractor shall provide innovation as a core component of every task. The contractor's management and employees shall require a constant focus on innovation. The contractor shall provide subject matter experts that are technology leaders in their discipline. It is anticipated that these technology leaders shall publish papers and speak at conferences as representatives of NASA. The Ames campus and its involvement with NASA activities provides a wide range of opportunities which technology leaders can identify as suitable for the application of innovative approaches and emerging technologies.

C.3.1.6.1 IT Security Innovation

The contractor shall provide bilingual staff with the capability to decode and reverse engineer custom code any malware written in English and languages other than English.

C.3.1.6.2 Cloud Computing

The Contractor shall provide expert staff to support the operation of NASA cloud computing environments and R&D to advance its capability. Specialists will be required in the areas of compute, storage, security, networking, virtualization, database management systems, capacity planning, performance tuning, resource accounting, web application platforms, and selected web applications. The Contractor shall provide staff experienced in the development and support of large, dynamically scalable compute and storage configurations spanning geographic locations and operating thousands of diverse workloads using a metered, utility-like delivery model. The Contractor shall support R&D to develop and deliver the cloud capabilities required to meet the needs of NASA's missions. The Contractor's efforts in this area shall provide NASA scientists with high performance cloud Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) capabilities.

C.3.1.6.3 Emerging Network Technology

The contractor shall provide support for network research, technology investigations, and the prototyping of new and emerging network technology in collaboration within NASA and outside organizations. The contractor shall have the capability to support NASA's implementation of emerging network technologies by satisfying requirements related to and including, but not limited to:

- advanced network technologies,
- managing agency customer requirements for advanced networking,
- exploring new network technologies, and
- exploring and implementing methods and protocols for increased network capacity (e.g., 40-100 Gbps).

The contractor shall possess a diverse capabilities set which allows it to excel in the support of ARC's efforts to embrace emerging network technologies. This skills set includes, but is not limited to, expertise in the following areas:

- support to High End Computing (HEC),
- performance of jumbo frame testing,
- IPv6 dynamic addressing assignment and configuration,
- making improvements to the fidelity of Netflow network monitoring,
- evaluating and testing 10 GigE firewalls and 10GigE IDS/IPS,
- supporting a multi-site Federal Cloud Computing test bed,
- providing dynamic reconfigurable network interfaces for flexible line-speed packet processing and network virtualization to enable flexible allocation of network infrastructure, and
- managing Infiniband over Wide Area Networks (WAN).

The research performed under this area will enable increased capability such as new approaches to enable applications to leverage increased network capacity for the NASA corporate local area network (LAN) and to meet mission requirements. The contractor shall coordinate technology transfers from this group to the groups managing the operations NASA WAN/LAN in support of the HQ OCIO and the Ames Internet Exchange (AIX).

C.3.1.6.4 Evaluation of New and Emerging IT Security Tools and Technology

The contractor shall be responsible for researching emerging and new IT Security threats, trends, and technology. The contractor should be responsible for researching IT Security threats that are being seen in other Federal entities as well as other commercial entities that may be targets of the latest threats. The Contractor should be a Subject Matter Expert in the field of IT Security and be capable of collaborating with other Agencies on the latest technologies they may be using to combat the latest "unseen" threats.

C.3.1.7 Outreach/Informational Systems and Support

This information technology area is dominated by rich content that must to be distributed efficiently and effectively to customers internal and external to ARC, which includes other NASA centers, other Government Agencies, and a diverse group of public and private sector individuals and entities.

C.3.1.7.1 Customer Support

The Contractor shall provide products and services to assist customers with basic use of equipment and applications and provide prompt response and resolution to user problems. Services include establishing and maintaining a call support center/help desk response plan, a response team, and a continuous improvement plan based on customer feedback and benchmarking. The contractor is responsible for tracking and following through on all Customer problems or concerns, including those which involve other contractors, thus insuring that that neither inter- nor intra-contract issues prevent customer problems from being addressed. The contractor is also responsible for providing Customer Relationship Managers to act as customer advocates relative to services and products provided through the CIO's organization.

The Contractor shall provide technical support and coordination to ensure effective and efficient IT training, including defining requirements; identifying potential sources for required products and services; designing, developing, and updating relevant training materials; scheduling, coordinating, and conducting relevant training classes; and assessing relevant technologies and technical approaches to improve training effectiveness.

C.3.1.7.2 IT Security Outreach, Training and Communications

The contract shall provide support in developing IT Security education sessions that may include Birds Of a Feather, town hall meetings, and All Hands meetings. The contractor may be required to lead or help develop training sessions to end-users, system administrators, CSOs, and Directorate Heads.

C.3.1.7.3 Library Systems

The Contractor shall provide for the design, development, installation, maintenance, operations, upgrades, configuration management, archiving, customer support, and security of library computer systems and related applications, including tracking systems for technical reports and data.

C.3.1.7.4 Conference/Presentation/Advocacy Support

The Contractor shall provide IT support of products and services associated with supporting internal and external conferences, presentations, or other public events that support, describe, and/or advocate ARC Missions, Programs, and Projects such as scientific proceedings or formal programmatic meetings. The IT Contractor staff shall develop and/or acquire presentation materials as well as coordinate, logistically prepare for, and conduct such events as needed.

C.3.2 Management and Administration

The Contractor shall utilize best practices throughout its management and administrative activities in order to provide the best value while meeting the defined requirements. The Contractor shall develop and implement best practices in a useful timeframe. Specifically, the Contractor shall be cognizant of and employ best practices when practical in all relevant management areas including personnel management, contract management, project management, software management, facility management, safety, and security.

C.3.2.1 Management Structure

The Contractor shall provide a management structure to effectively manage a professional and technical work force engaged in a wide range of IT-related services and development activities. The Contractor shall have organizational structure, procedures, and administrative support functions to effectively and efficiently manage the work performed under this contract. The management and administrative structure shall provide a single point of contact for interface with the Contracting Officer's Technical Representative (COTR) and shall provide procedures and management supervision to ensure compliance with applicable Government regulations for all material and work performed under this SOW.

C.3.2.2 Task Management

Each task shall have a Task Manager (TM) who shall be the single point of contact to the Task Requester (TR). The Contractor shall ensure that all task plans clearly identify all products and services that the Contractor is responsible for delivering or providing. When appropriate, subtasks may be subdivided into work assignments.

C.3.2.3 Software Management

Software management shall include the design, development, implementation, modification, maintenance, and operations of software algorithms, applications, and tools. Customers include individual users, local work groups, ARC-wide functions, and extended work groups that have members at other NASA Centers, in other parts of the U.S. Government, in academia, and in industry. Software management issues shall include standards, reuse, training, upgrades, compatibility, licensing, intellectual property rights, and security.

The Contractor shall be cognizant of and employ best software practices. Before developing software, the Contractor shall first determine if there is a more cost effective solution such as acquiring reusable software from ARC sources or other NASA or U.S. Government sources, or purchasing commercial off-the-shelf software (COTS).

The Contractor shall maintain software libraries. The Contractor shall make use of these libraries by utilizing reusable software before any software development occurs and by contributing new software to the libraries.

C.3.2.4 Other Direct Charges

It is anticipated that substantial quantities of hardware, software and/or subcontracted activities shall be purchased by the Contractor and billed under this award as other direct costs (ODCs). Other ODCs may include training, travel, and other miscellaneous expenses. Allocability and allowability of ODCs and related indirect charges shall be governed by the related ODC clauses in the contract.